Cryptographic Practices within Jacobite Diplomatic Networks (1715–1745): A Typology of Ciphers and Keys in Wartime

Camille Rocher
Université Bordeaux Montaigne
19 esplanade des Antilles
33607 Pessac, France
Camille.rocher@u-bordeaux-montaigne.fr

Abstract

This paper examines cryptographic practices within Jacobite diplomatic networks between 1715 and 1745 through the systematic analysis of a corpus of 57 cipher keys among the 318 ones preserved in the Stuart Papers. While Jacobite correspondence has been studied from political perspectives, the cipher keys themselves have rarely been considered as historical objects deserving systematic analysis. Focusing on periods of intense military and diplomatic activity, this study investigates the structure, typology, and circulation of cipher keys used by James Francis Edward Stuart and his agents across Europe. This article proposes a typology based on the combination of cryptographic features observed in the corpus and hybrid systems. A frequency-based analysis highlights recurrent patterns in key design and reveals a strong preference for hybrid systems combining jargon with monoalphabetic or homophonic substitution. The results show no clear correlation between the complexity of a cipher key and the status of the correspondents involved, suggesting that pragmatic constraints, such as usability, availability, and key reuse, played a decisive role in cryptographic choices. By foregrounding cipher keys as artefacts of communication, this study contributes to a better understanding of early modern cryptographic practices and sheds new light on the operational dynamics of Jacobite diplomatic networks during wartime.

1 Introduction

The study of early modern cryptography has increasingly shifted from modest-size ciphers toward broader analyses of cryptographic practices and systematic studies on the development of ciphers and the way they were encrypted (Megyesi, 2021; Ulbert, 2024). Among the materials preserved from this period, cipher keys occupy a central position, as they define not only the technical mechanisms of encryption but also reflect concrete practices of communication, secrecy, and risk management within political and diplomatic networks.

The Stuart Papers (c. 1689–1800), preserved at the Royal Archives in Windsor, contain an exceptional collection of cipher keys associated with Jacobite correspondence. These keys were used by James Francis Edward Stuart and members of his political and diplomatic networks operating across Europe. While Jacobite correspondence has been studied from political and diplomatic perspectives, the cryptographic dimension of these materials, and particularly the cipher keys themselves remains largely unexplored.

This article examines a corpus of 57 Jacobite cipher keys dating from 1715 to 1745, focusing on their structure, typology, and usage. In doing so, the study contributes to ongoing discussions in historical cryptology regarding the practical and contextual dimensions of cipher key design.

2 Historical Context

In 1689, following what is known in British historiography as the “Glorious Revolution” of 1688, James II and VII (1633–1701), who had been deposed from the thrones of England and Scotland, sought refuge in France at the court of Louis XIV, accompanied by approximately 40,000 supporters. This event marked the beginning of a prolonged struggle to recover the English and Scottish crowns, successively led by James II and VII and later by his descendants:

first his son James Francis Edward Stuart (1688–1766), known as the Old Pretender, and then his grandson Charles Edward Stuart (1720–1788), the Young Pretender. They were supported in their efforts by those who remained loyal to the Stuart dynasty, commonly referred to as the Jacobites (Pittock, 1998).

In order to advance their claims, the Jacobites needed to secure financial resources, troops, and arms. One of the primary means of achieving this was by seeking international support from foreign monarchies, particularly during periods of heightened geopolitical tension. As a result, several invasion attempts were launched in the context of major European conflicts, including the rising of 1715, shortly after the War of the Spanish Succession (1701–1714) and during the Great Northern War (1701–1721), as well as the projected invasion of 1717 and the failed landing of 1719, which coincided with the War of the Quadruple Alliance (1718–1720). The final and most significant attempt took place in 1745, during the War of the Austrian Succession (1740–1748) (Szechi, 2019).

3 Sources and Corpus

This work is based on the *Stuart Papers*, both the volume dedicated to cipher keys[1] and the correspondence between the Jacobite agents across Europe and the central power in periods of conflicts, meaning between September 15, 1715 and June 29, 1719[2], and January 1st, 1744 to August 8, 1745[3]. This period represents a sample of 57 keys preserved in the dedicated volume. This choice was made to be able to compare the keys given to the different agents, their use, and the possible keys missing from the register.

4 Analysis of Cipher Keys

4.1 Terminology and Typology

A cipher key defines the process by which plaintext elements are replaced with ciphertext equivalents in order to produce encrypted messages. The following terminology refers exclusively to the encryption systems identified in the sample of keys analysed in this study. Jargon (J) is a specific type of nomenclor in which a plaintext word is replaced with a ciphertext word rather than with a ciphertext character. Such substitutions usually concern personal names, geographical locations, or politically sensitive terms (Figure 1). Such substitutions usually concern nomenclator elements, most commonly personal names, geographical locations, or politically sensitive terms.

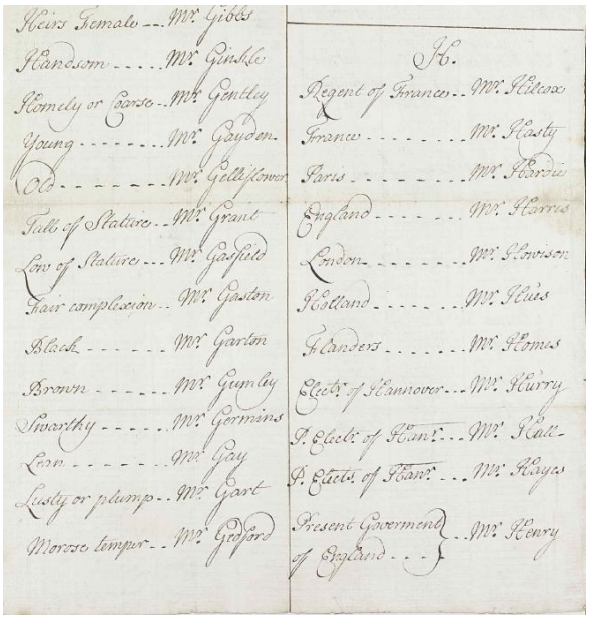

Figure 1. Example of jargon (RA SP/MAIN/5, f. 41)

Cipher keys that rely solely on nomenclators (N) encrypt plaintext elements using two- or three-digit codes assigned to a fixed list of words (Figure 2). Monoalphabetic substitution (M) assigns to each plaintext character a single ciphertext element. Homophonic substitution (H) allows a single plaintext element to be represented by several distinct ciphertext elements, in order to flatten frequency distributions and resist statistical attack. Polyalphabetic substitution (P) uses several substitution alphabets in alternation, typically governed by a keyword or a fixed pattern, so that the same plaintext character can be encrypted differently depending on its position in the message (Kahn, 1996). To complexify decryption, the most frequently occurring plaintext characters or words in a language might have several corresponding ciphertext characters. Cipher elements may be either fixed-length, in which all regular ciphertext elements consist of the same number of digits, or variable-length. While most of the surviving cipher keys used 3-digits ciphertext elements, some used ciphertext

[1] Royal Archives, Windsor, Stuart Papers, BOX/5, 290 keys, 992 folios.

[2] RA SP/MAIN/5 to RA/SP/MAIN/43.

[3] RA SP/MAIN/255 to RA/SP/MAIN/266.

elements that were between one and four digits long. Within the present corpus, all ciphertext elements are composed exclusively of words or numbers; no graphic symbols are used. Some keys also include dedicated ciphertext elements for punctuation marks. A final category concerns the use of nulls (Figure 2), that is, cipher elements without semantic value, which may serve either to introduce meaningless content or to cancel neighboring ciphertext elements. Those elements usually come under specific instructions of use. Since the creation of a new key was both tedious and time-consuming, already-existing ones were sometimes reused; either in full or with minor adaptations.

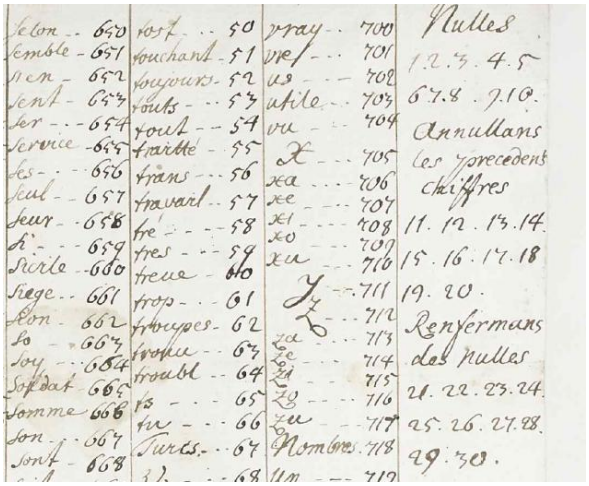

Figure 2. Example of a display of 2 and 3-digits code followed by nulls (RA SP/BOX/5, f. 45).

Rather than treating these techniques as mutually exclusive, this study adopts a combinatorial typology, in which each key is classified according to the set of cryptographic features it incorporates. This approach reflects the hybrid nature of early modern cipher keys and allows for meaningful comparison between systems of varying complexity while preserving their internal structure. This is similar to what is found in other early modern times keys (Megyesi et al., 2024).

4.2 Statistical analysis

A frequency-based analysis was conducted to identify recurring patterns and usage of cipher keys within the corpus. Rather than aiming at statistical exhaustiveness, this approach seeks to highlight tendencies in the distribution of cryptographic features and the relative complexity of the keys employed (Figure 3).

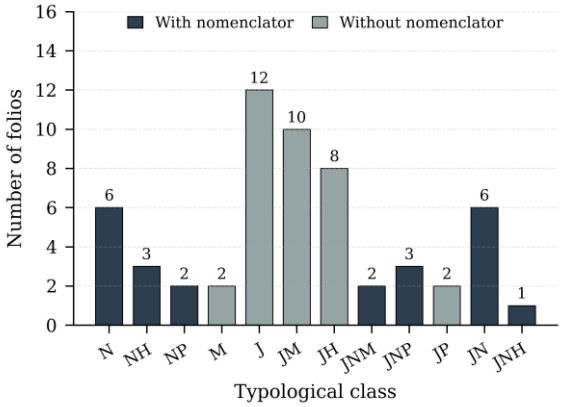

Figure 3. Distribution of cipher key types

The corpus is dominated by cipher keys relying partially or fully on substitution-based systems. Jargon encryption appears as the most frequent technique. However, in the majority of cases, this system is combined with two or more cryptographic features, such as monoalphabetic substitution, or nomenclator cipher, resulting in hybrid cipher keys rather than strictly homogeneous designs. Although sole nomenclators are less frequent than other substitutions, it appears in keys with a significantly higher number of entries (Figure 4).

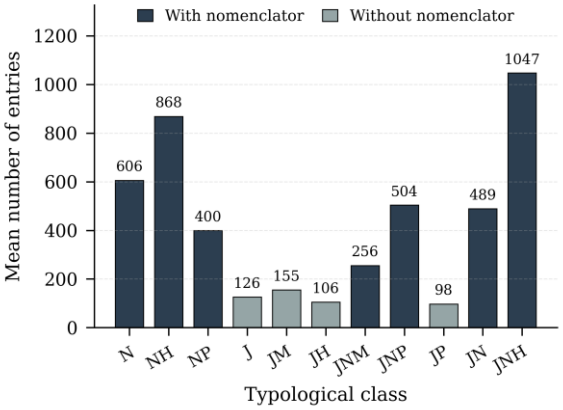

Figure 4. Number of entries per cypher key

This association indicates a tendency to reinforce encryption strength when the volume or importance of encrypted information increased. Conversely, keys with very limited lexical content tend to rely on substitution schemes, likely reflecting constraints of usability and the need for rapid deployment.

The most found system is a combination of homophonic substitution and nomenclator. This hybridization allows the agents greater autonomy and flexibility in the information they were allowed to transmit and the way they could

encrypt it, while allowing for greater complexity in encryption and thus limiting the risk of decryption by adversaries.

At the current stage of analysis, no clear correlation can be established between the structural complexity of a cipher key and the specific individuals or correspondents between whom it was used. While some highly elaborate keys are associated with prominent figures or sensitive exchanges (e. g. James Stuart or his secretary the duke of Mar), similarly complex systems also appear in more routine correspondence. This absence of a straightforward relationship suggests that factors other than individual status, such as practical constraints, availability of keys, or habits of reuse may have played a determining role in the choice of encryption methods.

4.3 Key Reuse and Circulation

Beyond their internal structure, cipher keys must also be understood as objects in circulation within communication networks. The analysis of the Jacobite corpus reveals that the production of cipher keys did not necessarily follow a strict logic of uniqueness. Instead, pragmatic considerations often governed key management.

At least three explicit cases of cipher key reuse have been identified within the corpus. In these instances, the same key appears to have been used over extended periods or shared between multiple correspondents. Such practices suggest that the creation of new keys was constrained by material, logistical, or cognitive factors. Copying, distributing, and memorising a key required time and effort, particularly within transnational networks operating under conditions of secrecy.

Beyond these clear cases, structural similarities observed across several keys raise the possibility of partial reuse or borrowing of cryptographic components, such as identical substitution alphabets or closely related nomenclator entries. While the present analysis does not allow for a definitive identification of systematic reuse, these patterns point toward a repertoire-based approach to cryptographic practice, in which pre-existing and trusted models were adapted rather than replaced.

Nine keys were addressed to two or more correspondents simultaneously, indicating that they were designed from the outset for collective use within sub-networks. This dimension of cryptographic practice deserves further investigation, particularly with regard to the geography and social composition of these sub-networks.

5 Conclusion & Future Works

Future research could include the transcription of all the cipher keys already identified, following the methodology developed by Tudor (2019), in order to enable a comprehensive analysis of the topics encrypted in Jacobite ciphers, such as the distribution and prominence of place names, personal names, and sensitive terms. Patterns of cipher reuse could also be explored using statistical methods, while the frequency of key usage in surviving correspondence represents another promising line of inquiry. Finally, the work of Tudor, Megyesi, and Láng (2020) on the automatic extraction of cipher key structures may offer valuable perspectives for further development.

References

David Kahn. 1996. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, New York.

Beáta Megyesi, Benedek Láng, Nils Kopal, Vasily Mikhalev, Crina Tudor, and Michelle Waldispühl. 2024. A Typology for Cipher Key Instructions in Early Modern Times. In *Proceedings of the 7th International Conference on Historical Cryptology,* HistoCrypt24, pages 183-193. Linköping University Electronic Press.

Beáta Megyesi, Crina Tudor, Benedek Láng, Anna Lehofer, Nils Kopal, Karl de Leeuw, and Michelle Waldispühl. 2024. Keys with Nomenclatures in the Early Modern Europe. In *Cryptologia*, 48(2), pages 97-139. Linköping University Electronic Press.

Beáta Megyesi, Crina Tudor, Benedek Láng, Anna Lehofer, Nils Kopal, and Michelle Waldispühl. 2022. What Was Encoded in Historical Cipher Keys in the Early Modern Era? In *Proceedings of the 5th International Conference on Historical Cryptology*, HistoCrypt22, pages 159-167. Linköping University Electronic Press.

Beáta Megyesi, Crina Tudor, and Benedek Láng, Anna Lehofer. 2021. Key Design in the Early Modern Era in Europe. In *Proceedings of the 4th International Conference on Historical Cryptology*, HistoCrypt21, pages 121-130. Linköping University Electronic Press.

Beáta Megyesi. 2020. Transcription of Historical Ciphers and Keys. In *Proceedings of the 3rd International Conference on Historical Cryptology*, HistoCrypt20, pages 106-115. Linköping University Electronic Press.

Murray Pittock. 1998. *Jacobitism.* Macmillan Press Ltd, Basingstoke, UK.

Daniel Szechi. 2019. *The Jacobites: Britain and Europe.* Manchester University Press, Manchester.

Crina Tudor, Beáta Megyesi, and Benedek Láng. 2020. Automatic Key Structure Extraction. In Proceedings *of the 3rd International Conference on Historical Cryptology*, HistoCrypt20, pages 146-152. Linköping University Electronic Press.

Crina Tudor. 2019. *Studies of Cipher Keys from the 16th Century: Transcription, Systematisation and Analysis*. Master thesis in Language Technology, Uppsala University, Sweden.

Jörg Ulbert. 2024. Le chiffre diplomatique français au dix-huitième siècle. In Sébastien Drouin and Sébastien Côté (ed.), *Secrets et surveillance épistolaires dans l'Europe du dix-huitième siècle*, pages 1-17. Voltaire Foundation in association with Liverpool University Press, Liverpool, UK.